REMARKS

Applicant thanks the Examiner for the careful review of this application. Claims 9 and 18-20 were amended to clarify aspects of the present invention. Claims 1-8, 10-17 and 21-32 were canceled without prejudice. Therefore, claims 9 and 18-20 remain pending in this application.

SPECIFICATION OBJECTION

The specification was objected to as failing to provide proper antecedent basis for the claimed subject matter. Specifically, the Examiner is objecting to the use the phrase 'Hensle lifting' in the claims. Applicant respectfully traverses the Examiner's finding for lack of support for the claimed subject matter. However, Applicant has canceled all claims that use the phrase 'Hensle lifting' and respectfully submits that the objection to the specification is now moot.

REJECTIONS UNDER 35 U.S.C. § 112, FIRST PARAGRAPH

Claims 1, 24-26 and 31-32 were rejected under 35 U.S.C. § 112, first paragraph as failing to comply with the enablement requirement. Applicant respect traverses. However, in the interests of expedited prosecution, Applicant has canceled claims 1, 24-26 and 31-32 and all dependent claims thereof. Therefore, the rejections of claims 1, 24-26 and 31-32 are now moot. Applicant respectfully reserves the right to introduce claims of an equivalent scope in this or a continuing application.

REJECTIONS UNDER 35 U.S.C. § 112, SECOND PARAGRAPH

Claims 1-32 were rejected under 35 U.S.C. § 112, second paragraph as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. Applicant respectfully traverses.

Again, in the interests of expedited prosecution, Applicant has canceled claims 1-8, 10-17 and 21-32 and the rejections of those claims are now moot. Applicant also reserves the right to re-introduce claims of an equivalent scope in this or a continuing application.

Regarding claim 9, Applicant has folded the limitations of dependent claim 13 into independent claim 9. Additionally, all occurrences of "RSA" has been removed and the phrasing "the private key is a function of two random numbers" has been amended to --the private key is a function of two randomly generated numbers such that $<r_1, r_2>$ satisfies $d=r_1 \mathrm{mod}(p-1)$ and $d=r_2 \mathrm{mod}(q-1)$--. Furthermore, "the RSA key" has also been amended to --the public key-- and "separating cipher-text moduli of the two distinct prime numbers" was also changed to --separating cipher-text moduli of the two distinct prime numbers, wherein cipher-text moduli refers to a mod(p,q)--. Finally, all occurrences of "efficiency" have been amended to state that the time to complete a particular task is decreased as a result of the preceding operations- for example, decryption time.

Regarding claims 18-20, each of these claims have been made independent by folding the limitations of independent claim 17 into each formerly dependent claim. Additionally, similar amendments that were made to claim 9 were also added to claims 18-20. Specifically, similar amendments were made regarding the rejections pertaining to the use of "RSA" encryption, defining the manner of how random numbers are generated and all occurrences of efficiency were changed to a time-based limitation to describe how the present invention improves upon the deficiency of prior art methods of encryption / decryption.

Withdrawal of the rejections of claims 9 and 18-20 is respectfully requested.

REJECTIONS UNDER 35 U.S.C. § 103(a)

Claims 1-5, 8, and 15 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Network Security Essentials: Applications and Standards by Stallings in view of Handbook of Applied Cryptography by Menezes and "Homework 4 with Extensive Hints" by Immerman and "Cryptalysis of Short RSA Secret Exponents" by Wiener.

Claims 9-12 and 29-30 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of "Twenty years of attacks on the RSA Cryptosystem" by Boneh.

Claim 14 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Boneh and further in view of Collins (U.S. Patent No. 5,848,159).

Claim 16 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Boneh in view of Stallings.

Claims 17 and 27-28 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Stallings in view of Menezes, Immerman, Weiner and "Fast RSA-type cryptosystem modulo of $p^k q$" by Takagi.

Claim 24 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Menezes in view of Takagi and further in view of Stallings and Aoki (U.S. Patent No. 6,578,061.

Claims 25 was rejected under 35 U.S.C. § 103(a) as being unpatentable over Boneh in view of Stallings, Takagi and Aoki.

Claims 26 and 31-32 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Boneh in view of Stallings, Takagi, Aoki and Collins.

Stallings apparently discloses a white paper on major concepts in network security, applications and standards.

Menezes apparently discloses various methods for encrypting data.

Immerman apparently discloses various illustrative examples of theorem proofs as they relate to encryption.

Wiener apparently discloses a description of a cryptanalytic attack on the use of short RSA secret exponents is described. This attack makes use of an algorithm based on continued fractions which finds the numerator and denominator of a fraction in polynomial time when a close enough estimate of the fraction is known. The public exponent *e* and the modulus *pq* can be used to perhaps create an estimate of a fraction which involves the secret exponent *d*. The algorithm based on continued fractions uses this estimate to possibly discover sufficiently short secret exponents. For a typical case where $e < pq$, *GCD*(p-1, q-1) is small, and *p* and *q* have approximately the same number of bits, this attack will perhaps discover secret exponents with up to approximately one-quarter as many bits as the modulus. This attack poses no threat to the normal case of RSA where the secret exponent is approximately the same size as the modulus. This is because this attack possibly uses information provided by the public exponent and, in the normal case, the public exponent can be chosen almost independently of the modulus.

Boneh apparently discloses an overview of various methods used to attack RSA-type encryption.

Collins apparently discloses a method and apparatus are for public key encryption and decryption schemes that employ a composite number formed from three or more distinct primes. The encryption or decryption tasks may be broken down into sub-tasks to obtain encrypted or decrypted sub-parts that are then combined using a form of the Chinese Remainder Theorem to obtain the encrypted or decrypted value. A parallel encryption/decryption architecture is also disclosed.

Takagi apparently discloses a variant of RSA-type encryption using a modulo p^kq.

Aoki apparently discloses a method for permuting and dividing 16 pieces of k-bit data held in 4k-bit long registers T.sub.0. T.sub.1, T.sub.2 and T.sub.3, k being an integer, the data of each register T.sub.i is ANDed with a desired one of mask data (00ffff00), (ff0000ff), (0000ffff) and (ffff0000), and such ANDs are ORed to obtain desired permuted data.

Applicant respectfully traverses the 35 U.S.C. § 103(a) rejections of claims 1-5, 8-12, 14-17 and 21-32. In the interests of expedited prosecution, however, Applicant has canceled claims 1-5, 8, 10-12, 14-17 and 21-32 and reserves the right re-introduce claims of an equivalent scope into this or a continuing application. The rejections of claims 1-5, 8, 10-12, 14-17 and 21-32 is therefore moot. Regarding claim 9, the limitations of dependent claim 13 were folded into independent claim 9. As claim 13 was not subject to a 35 U.S.C. § 103(a) rejection, Applicant respectfully submits that the rejection of claim 9 is also moot as a result.

CONCLUSION

Applicant believes that all pending claims are allowable and a Notice of Allowance is respectfully requested. The amendment was made to expedite the prosecution of this application. Applicant respectfully traverses the rejections of the amended claims and reserves the right to re-introduce them and claims of an equivalent scope in a continuation application.

If the Examiner believes that a conference would be of value in expediting the prosecution of this application, he is cordially invited to telephone the undersigned counsel at the number set out below.

Respectfully submitted,
PERKINS COIE LLP

J. P. Kudla

Dated: March 18, 2005

Jonathan P. Kudla
Reg. No. 47,724

Customer No. 22918
Perkins Coie LLP
P.O. Box 2168
Menlo Park, CA 94026
Telephone: (650) 838-4300